PERIODIC ORBITS OF LINEAR ENDOMORPHISMS ON THE 2-TORUS AND ITS LATTICES

MICHAEL BAAKE, JOHN A. G. ROBERTS, AND ALFRED WEISS

Abstract. Counting periodic orbits of endomorphisms on the 2-torus is considered, with special focus on the relation between global and local aspects and between the dynamical zeta function on the torus and its analogue on finite lattices. The situation on the lattices, up to local conjugacy, is completely determined by the determinant, the trace and a third invariant of the matrix defining the toral endomorphism.

1. Introduction

The iteration of a continuous mapping T of a compact space Ω into itself provides an example of a $\mathbb{Z}$-action on Ω and an important discrete dynamical system, usually written as (Ω, T). When Ω is a metric space, the system (Ω, T) is called *chaotic* when the periodic orbits of T are dense in Ω and when also a dense orbit exists, see [9] for details. In general, significant information about T is contained in the periodic orbits of T and in their distribution over Ω. Knowledge of the periodic orbits can be used to detect characteristic properties of T. For example, if T' represents another continuous mapping of Ω, then a necessary condition for T and T' to be topologically conjugate is that they share the same number of periodic points of each period (presuming these numbers are finite).

It is the aim of this paper to contribute to the structure of periodic orbits and related issues of conjugacy for the case of endomorphisms of the 2-torus, represented as usual by the action (mod 1) of an integer matrix $M \in \mathrm{Mat}(2,\mathbb{Z})$ on $\mathbb{T}^2 \simeq \mathbb{R}^2/\mathbb{Z}^2$. A well-studied subclass consists of the toral automorphisms, represented by elements of the group $\mathrm{GL}(2,\mathbb{Z})$, being the subgroup of matrices with determinant ± 1 within the ring $\mathrm{Mat}(2,\mathbb{Z})$. Particularly important are the hyperbolic ones (meaning that no eigenvalue is on the unit circle), which are often called *cat maps*. Since these are expansive, all periodic point counts are finite [41, Thm. 5.26]. Hyperbolic toral automorphisms are also topologically mixing and intrinsically ergodic, see [23, 41]. By the Bowen-Sinai theorem, compare [15, Thm. 2.2], this has the consequence that the integral of a continuous function over $\mathbb{T}^2$ equals its average value over the points fixed by M^m in the limit as $m \to \infty$.

The topological entropy of a hyperbolic toral automorphism $M \in \mathrm{GL}(2,\mathbb{Z})$ is given by $\log |\lambda_{\max}|$, where $\lambda_{\max}$ is the eigenvalue of M with modulus > 1. This is also the metric (or Kolmogorov-Sinai) entropy of M, and completely determines the dynamics up to metric isomorphism, compare [2]. This does not imply topological conjugacy though, and one important difference emerges from the periodic orbits, which live on a set of measure 0. Indeed, on $\mathbb{T}^2$, it is well-known that the periodic orbits of hyperbolic linear endomorphisms lie on the invariant lattices given by the sets of rational points with a given denominator n, also known as n-division points (see Section 2.2 for more). One of our main themes in this paper is the interplay between the periodic orbit statistics on a certain lattice (which we call *local statistics*) versus periodic orbit statistics on the union of all lattices (which we call *global statistics*). What determines when two cat maps have the same global statistics? What determines when two cat maps have the same local statistics on a certain lattice or on all lattices?

At the outset, it is worth saying that there have been many investigations by others into classifying the periodic orbits of cat maps, spread over a diverse range of the mathematics and physics literature, compare [21, 32, 24, 17, 19, 10][1] and further references given there. One motivation for this has come from the interest in spatial discretisations of dynamical systems, itself motivated by computer (screen) realisations of continuous phase spaces. The time of recurrence of a hyperbolic $M \in \mathrm{GL}(2,\mathbb{Z})$ on the toral rational lattice with denominator n is denoted by $\mathrm{per}(M,n)$, where this is the least common multiple of the periods present on the n-division points. The dependence of $\mathrm{per}(M,n)$ on n and related lower and upper bounds have been addressed in [17, 10, 28, 26, 18, 37]. In particular, the surprisingly low value of $\mathrm{per}(M,n)$ for some high values of n (which correspond to a very fine rational discretisation of the torus) has been investigated in [17, 10] where it is shown that $\mathrm{per}(M,n) \leq 3n$ (see [37] for refinements of this bound).

A strong motivation for studying cats maps on lattices comes from quantum mechanics, compare [21, 24, 25, 27, 28, 26, 18, 16]. As described in these references, quantum cat maps and their perturbations are built from (classical) cat maps and their perturbations *restricted to a particular rational lattice* (called the Wigner lattice in this instance). For this reason, properties of a cat map that manifest themselves only on some rational lattices, but not on others, can induce properties of the corresponding quantum cat map on some Wigner lattices, but again not on others. Important cases of this occur for symmetries or (time) reversing symmetries of a cat map, these being automorphisms of the torus that commute with the cat map, respectively conjugate it into its inverse. By way of illustration, it was shown in [7] that the first hyperbolic toral automorphism $A \in \mathrm{SL}(2,\mathbb{Z})$ which is not conjugate to its inverse in $\mathrm{GL}(2,\mathbb{Z})$ (which actually also excludes topological conjugacy to its inverse, compare [1]) occurs for trace 20. However, the global absence of time-reversal symmetry did not affect the statistics of the eigenvalues of the quantum cat map built from this example [25]. As explained there, this phenomenon is due to the fact that the quantum cat map retains (time) reversing symmetry because A is conjugate to its inverse mod n for any n and that the quantum cat map is constructed from the reduction of A mod n. Significantly, the conjugating matrix on each lattice depends on n, consistent with there being no global reversor. Recently, there has been quite some interest in dealing with this challenge of so-called pseudo-symmetries of quantum maps that are not quantisations of symmetries of the cat map on the torus, but instead are manifestations of local symmetries of the cat map restricted to some lattice [25, 27, 16].

[1] These investigations have used a variety of techniques. One is tempted to say, corrupting a proverb used by Mark Twain and others (`http://www.worldwidewords.org/qa/qa-mor1.htm`): *There's more than one way to skin a cat (map).*

When trying to sort cat maps by their global or local periodic orbit statistics, conjugacy is highly relevant. Conjugacy of $\mathrm{GL}(2,\mathbb{Z})$ matrices is another topic that has arisen in a broad variety of contexts and has been considered by many (see [40, 34, 3] and references therein). Conjugacy is determined by a triple of invariants, namely the determinant, the trace and one other invariant which can be related to ideal classes, representation by binary quadratic forms or topological properties [3]. Conjugacy in $\mathrm{GL}(2,\mathbb{Z})$ can also be completely decided by using the amalgamated free product structure of $\mathrm{PGL}(2,\mathbb{Z})$, which attaches a finite sequence of integers to each element which corresponds to its normal form as a word in the generators of the amalgamated free product [7]. Clearly, conjugate cat maps share both the same global period statistics and the same local statistics on each rational lattice (where the dynamics is conjugate via the localisation mod n of the global conjugating matrix). Also, cat maps that are just conjugate on a given rational lattice will share the same local statistics on that lattice. Being able to decide global and local conjugacies is thus clearly important, as the statistics is the same for all elements of a conjugacy class. But if two cat maps share the same local statistics on a given rational lattice, are they linearly conjugate on that lattice and what determines this?

The results of this paper will go some way towards answering the questions raised above. After recalling some well-known facts in Section 2, we look at periodic orbit counts for integer matrices in terms of zeta functions in Section 3. The dynamical zeta function for the global counts is described by Proposition 1, generalising a result of [15]. We then discuss a zeta function for the local periodic counts derived from the action of an integer matrix on a rational lattice. Theorem 1 relates the global and local zeta functions in a suitable limit. This is followed by an interpretation in terms of finite Abelian groups. Section 4 addresses the issue of local conjugacies of linear endomorphisms on rational lattices. The *matrix gcd*, which we define in Section 4.1, turns out to be a key quantity. It is preserved by $\mathrm{GL}(2,\mathbb{Z})$ conjugacy, so it provides a quick tool to see that two $\mathrm{GL}(2,\mathbb{Z})$ matrices with different matrix gcd are not conjugate on the torus. On the other hand, Theorem 2 and Corollary 3 show that two integer matrices that share the same determinant, trace and matrix gcd are linearly conjugate on all rational lattices of the torus. As an illustration of this result, consider our discussion above of quantum cat maps and time-reversal symmetry. The fact that any $M \in \mathrm{SL}(2,\mathbb{Z})$ shares determinant, trace and matrix gcd with M^{-1} means that the two matrices are conjugate on *all* rational lattices, though not necessarily by matrices that derive from one and the same matrix on the torus. This is nevertheless sufficient to guarantee that the associated quantum cat map has time reversal symmetry.

2. Notation and general setting

Here, we describe our setting and recall some well-known facts, tailored to the situation at hand. While we go along, we also introduce our notation and establish further connections with related topics in the recent literature.

2.1. **Counting orbits.** Consider a compact space Ω and some (continuous) mapping T of Ω into itself. Let $\mathrm{Fix}_m(T) := \{x \in X \mid T^m x = x\}$ be the set of fixed points of T^m. Of particular interest are the *fixed point counts*, defined as

$$a_m \,:=\, \operatorname{card}\{x \in \mathit{\Omega} \mid T^m x = x\} \,=\, \operatorname{card}(\operatorname{Fix}_m(T)), \tag{1}$$

which need not be finite in general. In many interesting cases, including all expansive homeomorphisms, this is the case though, including the toral endomorphisms without eigenvalues on the unit circle.

The quantity a_m has the disadvantage that one keeps recounting the contributions a_ℓ for all $\ell | m$. Clearly, the fixed points of *genuine* order m permit a partition into disjoint cycles, each of length m. If c_m is the number of such cycles, one thus has the relation

$$a_m \,=\, \sum_{d|m} d\, c_d . \tag{2}$$

An application of a standard inclusion-exclusion argument, here by means of the Möbius inversion formula from elementary number theory, results in the converse identity,

$$c_m \,=\, \frac{1}{m} \sum_{d|m} \mu\bigl(\tfrac{m}{d}\bigr)\, a_d , \tag{3}$$

where $\mu(k)$ is the Möbius function, compare [22, 33] and references therein for details.

Remark 1. Recall from [33] that a sequence $(a_m)_{m\in\mathbb{N}}$ of non-negative integers is termed *exactly realised* when it is the sequence of fixed point counts of a (continuous) dynamical system. This happens if and only if the derived sequence $(c_m)_{m\in\mathbb{N}}$ is a sequence of non-negative integers [33, Lemma 2.1]; see [42] for interesting examples other than toral endomorphisms and [31] for recent extensions of the concept. ◊

For later use, we briefly summarise some properties of the fixed point and orbit counts. Let $(a_m)_{m\in\mathbb{N}}$ and $(c_m)_{m\in\mathbb{N}}$ be a matching pair of such sequences, hence related as in Eqs. (2) and (3). The sequence of fixed point counts is called *periodic*, when an $n \in \mathbb{N}$ exists so that $a_{m+n} = a_m$ holds for all $m \in \mathbb{N}$. The least n with this property is called the *period* of the sequence $(a_m)_{m\in\mathbb{N}}$. The following consequences are standard.

Fact 1. *Let the non-negative integer sequences $(a_m)_{m\in\mathbb{N}}$ and $(c_m)_{m\in\mathbb{N}}$ satisfy Eq. (2). If a_m is periodic with period $n \in \mathbb{N}$, one has $c_m = 0$ for all $m > n$. Conversely, if only finitely many orbit counts c_m differ from 0, a_m is periodic, with period $n = \operatorname{lcm}\{m \in \mathbb{N} \mid c_m \neq 0\}$.* □

In extension of the usual practice for automorphisms, compare [23], we call a toral endomorphism $M \in \operatorname{Mat}(2,\mathbb{Z})$ *hyperbolic* when it has no eigenvalue on the unit circle $\mathbb{S}^1$. Recall that the standard 2-torus is $\mathbb{T}^2 \simeq \mathbb{R}^2/\mathbb{Z}^2$, where $\mathbb{Z}^2$ is the square lattice in the plane. It is a compact Abelian group, which can be written as $\mathbb{T}^2 := [0,1)^2$, with addition defined mod 1.

Fact 2. *If $M \in \operatorname{Mat}(2,\mathbb{Z})$ is hyperbolic, $\operatorname{Fix}_m(M) \subset (\mathbb{T}^2 \cap \mathbb{Q}^2)$ holds for all $m \in \mathbb{N}$.*

Proof. This can be shown by the concrete argument used in [23, Sec. 1.8, p. 44]. In essence, for any $m \in \mathbb{N}$, the equation $M^m x = x$ mod 1 means $(M^m - \mathbb{1})x = v$ for some integer vector v. Since 1 is not an eigenvalue of M^m, the integer matrix $M^m - \mathbb{1}$ is invertible, with rational inverse. Solving for x then gives the claim. □

This property motivates to look at periodic points of toral endomorphisms on certain subsets of $\mathbb{T}^2 \cap \mathbb{Q}^2$ as well.

2.2. **Invariant lattices on the 2-torus.** Recall that a *lattice* in a locally compact Abelian group is a co-compact discrete subgroup, such as $\mathbb{Z}^2$ in $\mathbb{R}^2$. For $\mathbb{T}^2$, a lattice simply means a discrete subgroup of it, which is then a *finite* Abelian group. The relevant lattices on $\mathbb{T}^2$ are

$$L_n := \left\{ \left(\tfrac{k}{n}, \tfrac{\ell}{n}\right) \mid 0 \leq k, \ell < n \right\}, \quad \text{for } n \in \mathbb{N}, \tag{4}$$

also known as n-division points, because they are invariant under toral endomorphisms.

Consider an integer matrix M that acts on $\mathbb{T}^2$ (meaning that it acts via matrix multiplication, evaluated mod 1). Clearly, one then has $ML_n \subset L_n$, and interesting information on the orbit structure of the toral endomorphism or automorphism ($\det(M) = \pm 1$) is contained in the distribution of its orbits on L_n. Alternatively, one can characterise L_n via

$$L_n = \{x \in \mathbb{T}^2 \mid nx = 0 \pmod 1\}. \tag{5}$$

Remark 2. When looking at the action of M on L_n numerically, it is usually easier to replace L_n by $\tilde{L}_n := \{(k, \ell) \mid 0 \leq k, \ell < n\}$, with the equivalent action of M defined mod n. This also applies to various theoretical arguments involving modular arithmetic. Consequently, we use L_n (with action of M mod 1) and $\tilde{L}_n$ (with action mod n) in parallel. $\Diamond$

From now on, we use the abbreviation $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ for the finite integer ring mod n, and $\mathbb{Z}_n^{\times} = \{1 \leq k \leq n \mid \gcd(k, n) = 1\}$ for its unit group. Let now $n \geq 2$ be arbitrary, but fixed. If we have a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$, its reduction mod n is still invertible in $\mathrm{Mat}(2, \mathbb{Z}_n)$, and thus an element of $\mathrm{Mat}(2, \mathbb{Z}_n)^{\times}$, the unit group within $\mathrm{Mat}(2, \mathbb{Z}_n)$. This group is often also called $\mathrm{GL}(2, \mathbb{Z}_n)$, though its elements need not have determinant ± 1.

Remark 3. A matrix $M \in \mathrm{Mat}(2, \mathbb{Z})$ that is not a toral automorphism (so $\det(M) \neq \pm 1$) may still be invertible on a given lattice L_n (or on $\tilde{L}_n$), meaning that M mod n is an element of $\mathrm{Mat}(2, \mathbb{Z}_n)^{\times}$. This happens precisely when $\det(M) \in \mathbb{Z}$ is relatively prime to n, which is equivalent to $\det(M) \in \mathbb{Z}_n^{\times}$ (where $\det(M)$ is taken mod n). $\Diamond$

When M is a toral automorphism, or a toral endomorphism with $\det(M) \in \mathbb{Z}_n^{\times}$, the invertible action of M on the finite set L_n induces a *permutation* of the n^2 elements of L_n, with one element ($x = 0$) always fixed. So, the induced permutation $\pi_M^{(n)}$ can either be viewed as an element of the symmetric group S_{n^2} or of S_{n^2-1}. The permutation is of finite order, which must divide $(n^2 - 1)!$ by Lagrange's theorem. The actual order of M on L_n is given by

$$\mathrm{ord}(M, n) := \gcd\{m \in \mathbb{N}_0 \mid M^m \equiv \mathbb{1} \mod n\}. \tag{6}$$

Clearly, $\mathrm{ord}(M, 1) = 1$ in this setting. When M is not invertible on L_n, the definition results in $\mathrm{ord}(M, n) = 0$; otherwise, $\mathrm{ord}(M, n)$ is the smallest $m \in \mathbb{N}$ with $M^m = \mathbb{1}$ mod n.

By an application of Fact 1, the orbit count sequence on L_n has vanishing entries beyond index $m = \mathrm{ord}(M, n)$. It is natural to define $a_\ell^{(n)} := \mathrm{card}\{x \in L_n \mid M^\ell x = x \pmod 1\}$ and

$$c_\ell^{(n)} := \mathrm{card}\{\text{cycles of } M \text{ on } L_n \text{ of length } \ell\}$$

as the induced fixed point and orbit counts on L_n, again mutually related as in Eqs. (2) and (3). It is not hard to see that

$$\operatorname{ord}(M,n) \;=\; \operatorname{per}(M,n) \;:=\; \operatorname{lcm}\{m \in \mathbb{N} \mid c_m^{(n)} \neq 0\}, \tag{7}$$

meaning that $\operatorname{per}(M,n)$ is the lcm of the lengths of the cycles on L_n. Clearly, we can only have $c_m^{(n)} \neq 0$ when m is a divisor of $\operatorname{per}(M,n)$.

When M is a toral endomorphism with $\gcd(\det(M),n) \neq 1$, it is not invertible on the lattice L_n. Consequently, not all points of L_n show up in periodic orbits of M, and one has 'pretails' to the periodic orbits (there is always at least one periodic orbit on L_n). Two matrices on L_n may thus share the same cycle structure there, but show different pretail patterns. As the latter give rise to a directed pseudo-graph on L_n (where 'pseudo' simply refers to the possibility of directed loops at a vertex), with the points of L_n as vertices and the directed edges derived from the action of M, it is reasonable to coin an adequate definition that covers both the case when M is invertible on L_n and when it is not.

Definition 1. We say that two matrices M and M' have the same *local statistics* on L_n when the induced directed pseudo-graphs on L_n are isomorphic as graphs. When M and M' are invertible on L_n, this is equivalent to saying that they have the same periodic orbit counts. Otherwise, this is equivalent to saying that they have the same periodic orbit counts plus isomorphic pretails between corresponding periodic orbits of the same length.

This definition shows that two matrices with different pretail structures for equal orbit counts would *not* have the same local statistics. Note that, when M and M' are invertible on L_n, they have the same local statistics if and only if their associated permutations $\pi_M^{(n)}$ and $\pi_{M'}^{(n)}$ are conjugate in S_{n^2}.

2.3. **Powers of 2×2-matrices.** Let $M \in \operatorname{Mat}(2,\mathbb{C})$ be a non-singular matrix, with $D := \det(M) \neq 0$ and $T := \operatorname{tr}(M)$. Define a two-sided sequence of (possibly complex) numbers p_m by the initial conditions $p_{-1} = -1/D$ and $p_0 = 0$ together with the recursion

$$\begin{aligned} p_{m+1} \;&=\; T p_m - D p_{m-1}, \quad \text{for } m \geq 0,\\ p_{m-1} \;&=\; \frac{1}{D}(T p_m - p_{m+1}), \quad \text{for } m \leq -1. \end{aligned} \tag{8}$$

This way, as $D \neq 0$, p_m is uniquely defined for all $m \in \mathbb{Z}$. Note that the sequence $(p_m)_{m\in\mathbb{Z}}$ depends only on the determinant and the trace of M. When $M \in \operatorname{Mat}(2,\mathbb{Z})$, one has $p_m \in \mathbb{Q}$, and $p_m \in \mathbb{Z}$ for $m \geq 0$. When $M \in \operatorname{GL}(2,\mathbb{Z})$, all p_m are integers.

Let us first note an interesting property, which follows from a straight-forward induction argument (in two directions).

Fact 3. *The two-sided sequence of rational numbers defined by the recursion* (8) *satisfies the relation* $p_m^2 - p_{m+1}p_{m-1} = D^{m-1}$, *for all* $m \in \mathbb{Z}$. □

Lemma 1. *Let* $M \in \operatorname{Mat}(2,\mathbb{C})$ *be non-singular. For* $m \in \mathbb{Z}$, *one has the relation*

$$M^m \;=\; p_m\, M - D p_{m-1}\, \mathbb{1}.$$

In particular, one has $M^{-1} = \frac{1}{D}(T\mathbb{1} - M)$.

Proof. The initial conditions $p_{-1} = -1/D$ and $p_0 = 0$ imply that the relation $M^0 = \mathbb{1}$ is matched. Let us first look at the positive powers of M. Assuming the claim to hold for some integer $m \geq 0$, we can use the Cayley-Hamilton theorem to proceed inductively. Indeed, from $M^2 = \mathrm{tr}(M)\, M - \det(M)\, \mathbb{1} = T M - D\, \mathbb{1}$, one finds with (8) that

$$\begin{aligned} M^{m+1} \;&=\; M^m\, M \;=\; p_m M^2 - D p_{m-1} M \\ &=\; (T p_m - D p_{m-1}) M - D p_m \mathbb{1} \;=\; p_{m+1} M - D p_m \mathbb{1}, \end{aligned}$$

which establishes the claim for all $m \geq 0$. The special relation for M^{-1} is just a reformulation of the inverse of a 2×2-matrix, while the statement about the negative powers follows from another induction argument, using the reverse recursion for the p_m with negative index. □

Remark 4. When $M \in \mathrm{Mat}(2,\mathbb{C})$ is *singular*, so $D = \det(M) = 0$, one can still meaningfully define the numbers p_m for all $m \geq 1$. In fact, they are then simply given by $p_m = T^{m-1}$, with $T = \mathrm{tr}(M)$. The formula from Lemma 1 simplifies to $M^m = p_m M = T^{m-1} M$, which is valid for all $m \geq 1$, while Fact 3 remains true for all $m \geq 2$. The numbers p_m are particularly useful to determine the periods $\mathrm{ord}(M,n)$ of Eq. (6). ◊

3. Dynamical zeta functions and periodic orbit statistics

To deal with combinatorial quantities such as the fixed point counts a_m, it is advantageous to employ generating functions. They provide a nice encapsulation of these numbers and permit the derivation of several asymptotic properties as well. Here, the concept of a *dynamical zeta function*, compare [36], is usually most appropriate. Consequently, given a matrix $M \in \mathrm{Mat}(2,\mathbb{Z})$, we set

$$\zeta_M(t) \;:=\; \exp\Bigl(\sum_{m=1}^{\infty} \frac{a_m}{m}\, t^m\Bigr), \tag{9}$$

where, from now on, $a_m := \mathrm{card}\{x \in \mathrm{Fix}_m(M) \mid x \text{ is isolated}\}$ is the number of *isolated* fixed points of M^m. We say more about this below.

Remark 5. The ordinary power series generating function for the counts a_m can be calculated from $\zeta_M(t)$ as $\sum_{m\geq 1} a_m t^m = t \frac{\mathrm{d}}{\mathrm{d}t} \log\bigl(\zeta_M(t)\bigr)$. The significance of the formulation used in Eq. (9) follows from the fact that it has a unique Euler product decomposition [36] as

$$\frac{1}{\zeta_M(t)} \;=\; \prod_{\text{cycles } \mathcal{C}} \bigl(1 - t^{|\mathcal{C}|}\bigr) \;=\; \prod_{m\geq 1} \bigl(1 - t^m\bigr)^{c_m}, \tag{10}$$

where $|\mathcal{C}|$ stands for the length of the cycle $\mathcal{C}$ and c_m is now the number of *isolated* cycles of M on $\mathbb{T}^2$ of length m, as determined from Formula (3). Consequently, the role of cycles in dynamics is similar to that of primes in elementary number theory. ◊

3.1. **Global considerations.** Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ and observe that $\mathrm{Fix}_m(M)$ is an Abelian group. In fact, it is a closed subgroup of $\mathbb{T}^2$. Consequently, when 1 happens to be an eigenvalue of M^m for some m, there is a continuous subgroup of fixed points of M^m, and one cannot have any isolated fixed points in addition, due to the group structure of $\mathrm{Fix}_m(M)$, see [6] for details. For a given toral endmorphism, any set $\mathrm{Fix}_m(M)$ is thus either finite (when 0 is an isolated fixed point) or a continuous submanifold of $\mathbb{T}^2$.

With hindsight, this motivates our definition in (9), and we now need to have an explicit formula for the number a_m of isolated fixed points of $M \in \mathrm{Mat}(2,\mathbb{Z})$ on $\mathbb{T}^2$. This is possible via a standard argument that involves areas of fundamental domains of planar lattices, compare [6, 15]. The subtorus case is treated in [6, Appendix].

Fact 4. *If $M \in \mathrm{Mat}(2,\mathbb{Z})$ is an arbitrary integer matrix, the number of isolated fixed points of M^m on $\mathbb{T}^2$ is given by*

$$a_m \,=\, \bigl|\det(M^m - \mathbb{1})\bigr|,$$

which is valid for all $m \in \mathbb{N}$. In particular, all these counts a_m and the corresponding cycle numbers c_m are finite. Moreover, whenever $a_m = 0$, no isolated fixed points exist, and one has subtori of fixed points instead. □

One can express a_m in terms of the numbers p_m from (8). Indeed, when $D = \det(M) \neq 0$, by inserting the formula from Lemma 1 and by also using Fact 3, one finds

$$\det(M^m - \mathbb{1}) \,=\, -p_{m+1} + D p_{m-1} + D^m + 1, \tag{11}$$

which is valid for all $m \geq 1$. By Remark 4, one can check that inserting $D = 0$ gives the correct formula also for $\det(M) = 0$, namely $\det(M^m - \mathbb{1}) = 1 - T^m$, with $T = \mathrm{tr}(M)$. With these formulae, one can determine the dynamical zeta functions of the isolated fixed points for many cases explicitly, compare [39, Sec. I.4] for an alternative approach.

Example 1. Let us start with $M \in \mathrm{Mat}(2,\mathbb{Z})$ being singular, and of trace T. One finds $\zeta_M(t) = 1/(1-t)$ for $T = 0$ and

$$\zeta_M(t) \,=\, \frac{1 - \mathrm{sgn}(T)t}{1 - |T|t} \tag{12}$$

for $T \neq 0$ (note the special role of $T = 1$, with $\zeta_M(t) = 1$, for the existence of subtori of solutions). The explicit derivation follows from Remark 4 and the standard power series identity (with $\varrho = 1$ as radius of convergence)

$$\log(1 - z) \,=\, -\sum_{m=1}^{\infty} \frac{z^m}{m}. \tag{13}$$

When $M = k\mathbb{1}$ with $k \in \mathbb{Z}$, a simple calculation results in

$$\zeta_M(t) \,=\, \frac{(1 - kt)^2}{(1-t)(1-k^2 t)}, \tag{14}$$

which is also valid for $M = \left(\begin{smallmatrix} k & b \\ 0 & k \end{smallmatrix}\right)$, with $b \in \mathbb{Z}$ arbitrary. If $k = 1$, we are back to a case with subtori of fixed points, again reflected by $\zeta_M(t) = 1$.

More generally, consider a non-singular upper triangular matrix of the form $M = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad \neq 0$, so that $\delta = \mathrm{sgn}(D) \neq 0$. Then, one finds the zeta function

$$\zeta_M(t) \,=\, \frac{\det(\mathbb{1} - \delta t M)}{(1-\delta t)(1 - \delta D t)} \,=\, \frac{(1-\delta a t)(1 - \delta d t)}{(1-\delta t)(1-\delta D t)}, \tag{15}$$

again using standard manipulations of power series. ◊

3.2. Zeta functions of toral automorphisms.

For $M \in \mathrm{GL}(2,\mathbb{Z})$, Fact 4 permits a derivation of the dynamical zeta function as follows, a special case of which was also given in [15].

Proposition 1. *Let $M \in \mathrm{GL}(2,\mathbb{Z})$ be hyperbolic, and define $\sigma = \mathrm{sgn}\bigl(\mathrm{tr}(M)\bigr)$. Then, with the coefficients $a_m = \mathrm{card}\{x \in \mathbb{T}^2 \mid M^m x = x \pmod 1\}$, the dynamical zeta function* (9) *of M on $\mathbb{T}^2$ is given by*

$$\zeta_M(t) \;=\; \frac{(1-\sigma t)(1-\sigma t\det(M))}{\det(\mathbb{1}-\sigma t M)} \;=\; \frac{(1-\sigma t)(1-\sigma\det(M)\,t)}{1-|\mathrm{tr}(M)|\,t+\det(M)\,t^2}.$$

In particular, $\zeta_M(t)$ is a rational function, with numerator and denominator in $\mathbb{Z}[t]$. The denominator is a quadratic polynomial that is irreducible over $\mathbb{Z}$. Its zero $t_{\min}$ closest to 0 *gives the radius of convergence of $\zeta_M(t)$, as a power series around* 0*, via $r_{\mathrm{c}} = |t_{\min}|$.*

Proof. Recall first from [36] that, for arbitrary matrices $A \in \mathrm{Mat}(n,\mathbb{C})$,

$$\exp\Bigl(\sum_{k=1}^{\infty}\frac{\mathrm{tr}(A^k)}{k}\,t^k\Bigr) \;=\; \frac{1}{\det(\mathbb{1}-tA)}, \tag{16}$$

with convergence for $|t| < 1/\varrho$, where ϱ is the spectral radius of A.

If M is hyperbolic, the general formula for the a_m from Fact 4 can be used to derive

$$a_m \;=\; \sigma^m\bigl(\mathrm{tr}(M^m) - (1+\det(M)^m)\bigr)$$

by observing that the two eigenvalues of A can be written as λ and $\det(A)/\lambda$. For the detailed argument, one may assume $|\lambda| > 1$ and check the different cases. Note that a hyperbolic toral automorphism is never of trace 0.

The formula for the zeta function now follows from (9) by inserting the expression for a_m and using the relation (16) together with the power series identity (13). The statement on the nature of the rational function is then clear. With $M \in \mathrm{GL}(2,\mathbb{Z})$, the denominator only factorises for $\mathrm{tr}(M) = 0$, $\det(M) = -1$ or for $\mathrm{tr}(M) = \pm 2$, $\det(M) = 1$, both cases being impossible for hyperbolic matrices. The result on the radius of convergence is standard. □

Example 2. Probably the best known hyperbolic toral automorphism is the one induced by the 'classic' or golden cat map

$$M \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

It has $\det(M) = -1$ and is thus orientation reversing (sometimes, as in [23], its square is used instead). From Proposition 1 or from [6], one obtains

$$\zeta_M(t) \;=\; \frac{1-t^2}{1-t-t^2} \;=\; \prod_{m\geq 1}\bigl(1-t^m\bigr)^{-c_m}$$

with $a_m = f_{m+1} + f_{m-1} - \bigl(1+(-1)^m\bigr)$ and c_m according to Eq. (3), see also entries `A001350` and `A060280` of [38]. Here, f_m are the Fibonacci numbers, defined by the recursion $f_{m+1} = f_m + f_{m-1}$, for $m \geq 0$, together with the initial condition $f_0 = 0$ and $f_{-1} = 1$. The first few terms of the counts are given in Table 1. As an aside, note that $\zeta_M(t) = 1 + \sum_{m=0}^{\infty} f_m t^m$, and one has $M^m = f_m\, M + f_{m-1}\,\mathbb{1}$, the latter being valid for all $m \in \mathbb{Z}$. ◊

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_m	1	1	4	5	11	16	29	45	76	121	199	320	521	841	1364
c_m	1	0	1	1	2	2	4	5	8	11	18	25	40	58	90

Table 1. Fixed point and orbit counts for the golden cat map.

Remark 6. In Example 2, when taken mod n, the powers M^m are periodic in m with period P_n, which are known as the *Pisano periods*, see entry `A001175` of [38]. The periods of the sequences $\big(a_m^{(n)}\big)_{m\in\mathbb{N}}$ divide P_n, but can be smaller, as happens for $n = 4$ (with 3 versus $P_4 = 6$) or for $n = 5$ (with 4 versus $P_5 = 20$). ♢

Let us return to our general discussion. From Proposition 1, it is clear that two hyperbolic $\mathrm{GL}(2,\mathbb{Z})$-matrices with the same trace and determinant possess the same dynamical zeta function, hence the same fixed point counts. The converse is slightly more subtle.

Corollary 1. *Let $M, M' \in \mathrm{GL}(2,\mathbb{Z})$ represent two hyperbolic toral automorphisms which have the same fixed point counts. Then, $\zeta_M(t) = \zeta_{M'}(t)$. This implies $\det(M') = \det(M)$ and either $\mathrm{tr}(M') = \mathrm{tr}(M)$ or $\mathrm{tr}(M') = -\,\mathrm{tr}(M)$, the latter together with $\det(M) = -1$.*

Proof. The claimed equality of the zeta functions is clear. As the denominator is irreducible over $\mathbb{Z}$ by Proposition 1, we get $\det(M') = \det(M)$ and $|\mathrm{tr}(M')| = |\mathrm{tr}(M)|$. Equating the numerators results in the two possibilities stated. □

Remark 7. The second possibility of Corollary 1 is realised by any orientation reversing $\mathrm{GL}(2,\mathbb{Z})$-matrix M together with $M' = -M$. One can also check this property by an explicit calculation, using Fact 4 in conjunction with Lemma 1 and Fact 3.

A concrete example is provided by the golden cat map (or Fibonacci matrix) $M = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ of Example 2. Since $-\mathbb{1}$ is a lattice symmetry for all L_n, it is clear that also the local statistics of M and $-M$ is the same on all lattices. ♢

The formula of Proposition 1 does not necessarily hold for the elliptic and parabolic elements of $\mathrm{GL}(2,\mathbb{Z})$. However, those cases can be derived from the formulas given in Example 1, and result, in our setting, in the dynamical zeta function for the *isolated* fixed points.

3.3. **Generating functions on lattices.**

Let us now consider a toral endomorphism M on the lattice L_n, for some $n \in \mathbb{N}$. It is clear that L_n is mapped onto itself under the action of M (mod 1). Alternatively, by Remark 2, we may consider $\tilde{L}_n$, and thus the action of the reduction of M mod n. Recalling that $\mathrm{card}(L_n) = \mathrm{card}(\tilde{L}_n) = n^2$, the following observation is obvious.

Fact 5. *Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ and $n \in \mathbb{N}$ be fixed. Then, only finitely many of the orbit counts $c_\ell^{(n)}$ on L_n can be non-zero, and the dynamical zeta function for the action of M on L_n has the property that*

$$Z_n(t) \,:=\, \frac{1}{\zeta_M^{(n)}(t)} \,=\, \prod_{\ell\geq 1} (1-t^\ell)^{c_\ell^{(n)}}$$

is a finite product and defines a polynomial in $\mathbb{Z}[t]$ of degree at most n^2. □

Note that the degree of $Z_n(t)$ can indeed be less than n^2. This happens whenever the action of M is non-invertible on L_n, which manifests itself in the existence of pretails to the actual orbits. Otherwise, Fact 5 can be sharpened as follows.

Proposition 2. *Let $M \in \mathrm{GL}(2,\mathbb{Z})$ or, more generally, let $\det(M)$ for $M \in \mathrm{Mat}(2,\mathbb{Z})$ be coprime with n, meaning that the reduction of M is an element of $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times} = \mathrm{GL}(2,\mathbb{Z}_n)$. Then, the dynamical zeta function $\zeta_M^{(n)}(t)$ satisfies*

$$\frac{1}{\zeta_M^{(n)}(t)} \, = \prod_{\ell \,|\, \mathrm{per}(M,n)} \bigl(1-t^{\ell}\bigr)^{c_\ell^{(n)}} \; =: \, Z_n(t),$$

where $Z_n(t) \in \mathbb{Z}[t]$ has degree n^2. In particular, with $N = \mathrm{per}(M,n)$, one has

$$\sum_{\ell \,|\, N} \ell \, c_\ell^{(n)} \, = \, a_N^{(n)} \, = \, n^2,$$

and the minimal period of the sequence $\bigl(a_m^{(n)}\bigr)_{m\in\mathbb{N}}$ is a divisor of N. □

Concerning the last statement, it is worthwhile to mention that the minimal period of the fixed point counts on L_n can actually be smaller than $\mathrm{per}(M,n)$, as we saw in Remark 6. Note that $(1-t)|Z_n(t)$ for all $n \geq 1$, since $x = 0$ is a fixed point of M on all L_n. Moreover, $m|n$ implies $Z_m|Z_n$. This induces a partial order on the polynomials Z_n, which permits us to consider the direct (or inductive) limit of them, considered within the ring of formal power series, $\mathbb{Z}[[t]]$, compare [20, Sec. 1]. In fact, one simply has

$$\varinjlim Z_n(t) \, = \, \lim_{n\to\infty} \mathrm{lcm}\{Z_1(t), Z_2(t), \ldots, Z_n(t)\},$$

where lcm stands for the least common multiple, which is well-defined here because the polynomial ring $\mathbb{Z}[t]$ is factorial, see [29]. It is clear by construction that this limit must divide $1/\zeta_M(t)$, the latter written out as an infinite Euler product and thus as an element of $\mathbb{Z}[[t]]$. In our setting, the formal power series have positive radius of convergence, so that one can also extract asymptotic properties of their coefficients by standard tools from complex analysis, compare [15, 20] for examples.

Theorem 1. *If $M \in \mathrm{Mat}(2,\mathbb{Z})$ is hyperbolic, one has $\varinjlim Z_n(t) \, = \, 1/\zeta_M(t)$.*

Proof. When M has no unimodular eigenvalue, Fact 4 gives a formula for the number of *all* fixed points of M^m, which is finite. It is clear that the finitely many fixed points of M^m are isolated. Viewing each polynomial $Z_n(t)$ as an element of $\mathbb{Z}[[t]]$, it is clear that

$$\varinjlim Z_n(t) \mid 1/\zeta_M(t),$$

where $1/\zeta_M(t)$ is written as the Euler product of (10), hence as an element of $\mathbb{Z}[[t]]$, which contains each $Z_n(t)$ as a factor. It remains to show that each factor $(1-t^m)^{c_m}$ of $1/\zeta_M(t)$ divides $Z_n(t)$ for some $n \in \mathbb{N}$ (and then also for all multiples n' of n).

Note that all fixed points of M^m lie in $\mathbb{Q}^2 \cap \mathbb{T}^2 \simeq \mathbb{Q}^2/\mathbb{Z}^2$ by Fact 2. Consequently, there must be some $n = n(m)$ such that all these fixed points are in L_n, which implies $(1-t^m)^{c_m}|Z_n(t)$. The claim now follows from the general structure of the direct limit. □

Remark 8. The direct limit does not exist for all matrices in $\mathrm{Mat}(2,\mathbb{Z})$. This relates to the observation that endomorphisms with subtori of fixed points of some order have no isolated fixed points of the same order, while the intersections with the lattices L_n are still finite sets. In this situation, $\zeta_M(t)$ encapsulates the isolated fixed point counts only (if any), while $Z_n(t)$ gradually explores also the non-isolated ones. ◊

3.4. **Group theoretic interpretation.** Both the torus $\mathbb{T}^2$ and its lattices L_n are compact Abelian groups (the latter even being finite). It is thus natural to also expect some group theoretic interpretation of counting orbits of a hyperbolic toral endomorphism M on these groups. Recall that

$$A_m \,:=\, \mathrm{Fix}_m(M) \,=\, \{x \in \mathbb{T}^2 \mid M^m x = x \ (\mathrm{mod}\ 1)\} \tag{17}$$

is a subgroup of $\mathbb{T}^2$, hence a *finite* Abelian group of order a_m due to the assumption of hyperbolicity. Knowing a_m, however, generally tells us rather little about A_m as a group. To improve on this, we employ the elementary divisor theorem for finite Abelian groups, compare [14, Thm. I.4.2] or [29, Ch. I.4.8]. To this end, consider

$$A^{(n)}_m \,:=\, A_m \cap L_n \,=\, \{x \in A_m \mid nx = 0 \ (\mathrm{mod}\ 1)\},$$

which defines a family of Abelian groups, with $a^{(n)}_m = \mathrm{card}\bigl(A^{(n)}_m\bigr) \le a_m$ and $A^{(n)}_m \subset A_m$. In fact, since we assume here that M has no eigenvalues on $\mathbb{S}^1$, one has $A_m = \bigcup_{n\in\mathbb{N}} A^{(n)}_m$.

Proposition 3. *The structure of the finite Abelian group A_m of* (17) *is completely determined by the numbers $a^{(n)}_m$ with $n \in \mathbb{N}$.*

Proof. Fix $m \in \mathbb{N}$, and write $G = A_m$. Choose an isomorphism

$$G \simeq \bigoplus_{i=1}^{s} \mathbb{Z}/p_i^{\ell_i}\mathbb{Z},$$

which exists by the elementary divisor theorem, with $s \in \mathbb{N}$; note that the primes p_i need not be distinct. Set $G(n) = A^{(n)}_m$ and $g(n) = a^{(n)}_m$, where $g(1) = 1$. In view of the elementary divisor theorem, it now suffices to show that, for each prime power p^r with $r \ge 1$, the power of p in

$$\frac{g(p^r)\, g(p^r)}{g(p^{r-1})\, g(p^{r+1})} \;=\; \frac{[G(p^r) : G(p^{r-1})]}{[G(p^{r+1}) : G(p^r)]}$$

equals the number of indices i so that $p_i = p$ and $\ell_i = r$. This follows from $g(p^r) = p^t$ where

$$t = \sum_{i : p_i = p} \min(r, \ell_i).$$

This uniquely specifies all elementary divisors. □

4. Global versus local conjugacy and orbit statistics

The determinant and the trace of an integer matrix are not changed under $\mathrm{GL}(2,\mathbb{Q})$ conjugacy. But for matrices $M \in \mathrm{Mat}(2,\mathbb{Z})$, it has been known for a long time that the determinant and the trace are neither a sufficient nor a maximal set of invariants (this goes back to contributions by Latimer, MacDuffee, Taussky and Rademacher – see [40, 3, 34] and references therein). There are various ways of deciding $\mathrm{GL}(2,\mathbb{Z})$-conjugacy, amounting to exploiting a third and final conjugacy invariant [4, 3, 7, 34]. It is clear that there are many interesting connections to class groups and class numbers of quadratic number fields, see [40] for details.

Example 3. Consider the two $\mathrm{GL}(2,\mathbb{Z})$-matrices

$$M = \begin{pmatrix} 3 & 10 \\ 1 & 3 \end{pmatrix} \quad \text{and} \quad M' = \begin{pmatrix} 3 & 5 \\ 2 & 3 \end{pmatrix},$$

which share $D = -1$ and $T = 9$. One can check explicitly that the integral matrices X which satisfy $MX = XM'$ are integral linear combinations of A and B, where

$$A = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

For each integer $n > 2$, one can find an X with $\det(X)$ coprime to n, so that the reductions of M and M' mod n are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate. However, when taken mod 5, $\det(X)$ is always congruent to 0, 2 or 3. Consequently, no X exists with $\det(X) = \pm 1$, whence M and M' are not conjugate in $\mathrm{GL}(2,\mathbb{Z})$. ◊

Obviously, two $\mathrm{GL}(2,\mathbb{Z})$-conjugate hyperbolic toral automorphisms do possess the same dynamical zeta function on $\mathbb{T}^2$, equivalently have the same sequence of fixed point counts. They also have the same local statistics on all lattices L_n. The latter statement follows from the observation that the conjugating $\mathrm{GL}(2,\mathbb{Z})$-matrix element leaves all L_n invariant and induces a local conjugacy on all of them. This is a particular case of a result for endomorphisms (recall Remark 3 and its preceding paragraph):

Fact 6. *Let $n \geq 2$ be an integer. If two matrices $M, M' \in \mathrm{Mat}(2,\mathbb{Z})$ are $\mathrm{GL}(2,\mathbb{Z})$-conjugate, their reductions mod n are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate.*

Proof. By assumption, we have $M' = AMA^{-1}$ for some $A \in \mathrm{GL}(2,\mathbb{Z})$, which mod n is turned into an equation of the same type within $\mathrm{Mat}(2,\mathbb{Z}_n)$, with $A \in \mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$. □

Conversely, if two hyperbolic matrices $M, M' \in \mathrm{Mat}(2,\mathbb{Z})$ share the same fixed point counts on all lattices L_n, they must also have the same fixed point counts on $\mathbb{T}^2$. If $M, M' \in \mathrm{GL}(2,\mathbb{Z})$, Corollary 1 implies that they have the same determinant. They also have the same trace if they are orientation-preserving (their traces may differ in sign if they are orientation-reversing). Even in the orientation-preserving case, the equivalence of local statistics for all n does *not* imply $\mathrm{GL}(2,\mathbb{Z})$-conjugacy. For instance, M and $M' = M^{-1}$ must have the same set of fixed point counts on all lattices L_n, as M^{-1} simply runs backwards through the orbits of M. But a hyperbolic toral automorphism need not be conjugate to its inverse:

Example 4. The two matrices

$$M = \begin{pmatrix} 4 & 9 \\ 7 & 16 \end{pmatrix} \quad \text{and} \quad M^{-1} = \begin{pmatrix} 16 & -9 \\ -7 & 4 \end{pmatrix} \tag{18}$$

with $D = 1$, $T = 20$ are *not* conjugate within $\mathrm{GL}(2,\mathbb{Z})$, as one can check by an explicit calculation [7] (in fact, this means they are not even topologically conjugate, see [8, Fact 1]).

Note that the companion matrix C for both M and M^{-1} is conjugate to its inverse:

$$C = \begin{pmatrix} 0 & -1 \\ 1 & 20 \end{pmatrix} \quad \text{with inverse} \quad C^{-1} = \begin{pmatrix} 20 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 20 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{19}$$

This means that C and its inverse are in yet another $\mathrm{GL}(2,\mathbb{Z})$ conjugacy class than M and M^{-1} (one can calculate that there are altogether 5 conjugacy classes for $D = 1$ and $T = 20$, compare [5, Ex. 17]). We thus see that the set of integer matrices with the same local statistics on all lattices L_n can encompass more than one matrix conjugacy class on $\mathbb{T}^2$. ◊

Two conjugate matrices possess equivalent orbit structures, including pretails of periodic orbits. In view of Remark 2, the following local property is then clear.

Fact 7. *Let $n \in \mathbb{N}$. When two integer matrices M and M' are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate, the corresponding toral endomorphisms have the same local statistics on the lattice L_n, in the sense of Definition 1.* □

In the remainder of this section, we answer the question when two integer matrices

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \tag{20}$$

from $\mathrm{Mat}(2,\mathbb{Z})$ are locally conjugate (mod n) for all n and hence possess the same local statistics (in the sense of Definition 1) on all lattices L_n. This will only depend on the determinant, the trace and a new invariant that we introduce next.

4.1. The matrix gcd.

Consider a 2×2-matrix M as in (20).

Definition 2. If $M \in \mathrm{Mat}(2,\mathbb{Z})$, the quantity

$$\mathrm{mgcd}(M) := \gcd(b, c, d-a),$$

is called the *matrix gcd* of M, or mgcd for short[2]. Here, we take the gcd to be a non-negative integer, and set $\mathrm{mgcd}(M) = 0$ when $b = c = d - a = 0$.

The last convention matches that of the ordinary gcd, and is compatible with modular arithmetic. The following consequence of this definition is obvious.

Fact 8. *For $M \in \mathrm{Mat}(2,\mathbb{Z})$, the following statements are equivalent:*

(a) *The matrix gcd satisfies* $\mathrm{mgcd}(M) = 0$.
(b) *$M = k\mathbb{1}$ for some $k \in \mathbb{Z}$.*
(c) *The minimal polynomial of M is of degree* 1.

Consequently, whenever $\mathrm{mgcd}(M) = r \in \mathbb{N}$, M cannot be a multiple of the identity, and its characteristic and minimal polynomials coincide. □

[2] A generalisation of the mgcd to $n \times n$ integer matrices, $n \geq 2$, is the quantity m of [12], which is used to describe the least normal subgroup in $\mathrm{GL}(n,\mathbb{Z})$ containing a given element.

There are various other useful properties of the matrix gcd. It is immediate that

$$\mathrm{mgcd}(-M) \;=\; \mathrm{mgcd}(M) \;=\; \mathrm{mgcd}(M^t) \tag{21}$$

holds for arbitrary $M \in \mathrm{Mat}(2,\mathbb{Z})$. Moreover, with $k \in \mathbb{Z}$, one has

$$\mathrm{mgcd}(kM) \;=\; k\,\mathrm{mgcd}(M) \quad \text{and} \quad \mathrm{mgcd}(M + k\mathbb{1}) \;=\; \mathrm{mgcd}(M). \tag{22}$$

Finally, if M is invertible, its inverse is $M^{-1} = \frac{1}{\det(M)} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Consequently, for all matrices $M \in \mathrm{GL}(2,\mathbb{Z})$, one has the relation

$$\mathrm{mgcd}(M^{-1}) \;=\; \mathrm{mgcd}(M) \tag{23}$$

in addition to (21).

Most significantly, the matrix gcd satisfies the following invariance property, which can be seen as a consequence of the close relationship to the theory of binary quadratic forms [43].

Lemma 2. *If $M, M' \in \mathrm{Mat}(2,\mathbb{Z})$ are two integer matrices that are conjugate via a $\mathrm{GL}(2,\mathbb{Z})$-matrix, one has $\mathrm{mgcd}(M') = \mathrm{mgcd}(M)$. In particular, the matrix gcd of Definition 2 is constant on the conjugacy classes of $\mathrm{GL}(2,\mathbb{Z})$.*

Proof. Assume $M' = AMA^{-1}$ with $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$. One can check by a straightforward calculation that this implies the linear equation

$$\begin{pmatrix} b' \\ c' \\ d'-a' \end{pmatrix} = \frac{1}{\det(A)} \begin{pmatrix} \alpha^2 & -\beta^2 & \alpha\beta \\ -\gamma^2 & \delta^2 & -\gamma\delta \\ 2\alpha\gamma & -2\beta\delta & \beta\gamma + \alpha\delta \end{pmatrix} \begin{pmatrix} b \\ c \\ d-a \end{pmatrix} =: N \begin{pmatrix} b \\ c \\ d-a \end{pmatrix},$$

where $N = N(A)$ is an integer matrix because $\det(A) = \pm 1$. As the primed quantities are then integer linear combinations of the unprimed ones, $\gcd(b,c,d-a)$ divides $\gcd(b',c',d'-a')$. It is easy to verify that $\det(N) = 1$, so that $N \in \mathrm{GL}(3,\mathbb{Z})$ and N^{-1} is an integer matrix as well (this can also be seen directly from observing that $M = A^{-1}M'A$ and hence $N(A^{-1}) = (N(A))^{-1}$). Consequently, our previous argument implies that $\gcd(b',c',d'-a')$ divides $\gcd(b,c,d-a)$ as well. Within $\mathbb{N}$, we thus obtain $\gcd(b',c',d'-a') = \gcd(b,c,d-a)$ as stated. This conclusion also holds when one gcd (and then also the other) vanishes, adopting the usual convention that $0|0$. The second claim is now obvious. □

Remark 9. Two integer matrices with different mgcd cannot be $\mathrm{GL}(2,\mathbb{Z})$-conjugate. Note, however, that M, M^{-1} and C of Example 4 all have mgcd $= 1$, but are in distinct $\mathrm{GL}(2,\mathbb{Z})$ conjugacy classes as discussed. ◊

4.2. **Local conjugacies and a binary quadratic form.** With a view to determining conjugacies on L_n, meaning conjugacy via $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$, consider the integer matrices

$$M \;=\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad C \;=\; \begin{pmatrix} 0 & -D \\ 1 & T \end{pmatrix} \tag{24}$$

with $D = \det(M)$ and $T = \mathrm{tr}(M)$. Here, C is the standard companion matrix for the characteristic polynomial

$$x^2 - Tx + D \tag{25}$$

of the matrix M. Let us assume that M is *not* a multiple of $\mathbb{1}$. To investigate possible conjugacies, let $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ be another integer matrix. It is easy to check that

$$MA \, = \, AC \quad \Longleftrightarrow \quad \begin{pmatrix} \beta \\ \delta \end{pmatrix} \, = \, M \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} . \tag{26}$$

Whenever this semi-conjugacy holds, one has

$$\det(A) \, = \, c\,\alpha^2 + (d-a)\alpha\gamma - b\,\gamma^2 \, =: \, Q_M(\alpha,\gamma), \tag{27}$$

which brings us in contact with the classic theory of binary quadratic forms.

In fact, the quadratic form Q_M is the key for a hierarchy of conjugacies. Clearly, M and C are $\mathrm{GL}(2,\mathbb{Q})$-conjugate if Q_M represents *some* $\mu \neq 0$. This is true unless $\mathrm{mgcd}(M) = 0$, which relates back to Fact 8. Whenever Q_M represents 1 or -1 (which then automatically implies α and β to be coprime), the matrices M and C are $\mathrm{GL}(2,\mathbb{Z})$-conjugate (this is one of the approaches to $\mathrm{GL}(2,\mathbb{Z})$-conjugacy taken in [3, 7]). When Q_M represents some $\mu \in \mathbb{N}$, and when $n \in \mathbb{N}$ is another integer that is relatively prime with μ, one has $\mu \in \mathbb{Z}_n^{\times}$, wherefore A is invertible in $\mathrm{Mat}(2,\mathbb{Z}_n)$, compare Remark 3, and the reductions of M and C mod n are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate.

The discriminant of the binary quadratic form Q_M of (27) is

$$\varDelta = (d-a)^2 + 4bc = (a+d)^2 - 4(ad-bc) = T^2 - 4D. \tag{28}$$

The form Q_M is called *primitive* when $\gcd(b,c,d-a) = 1$, which means $\mathrm{mgcd}(M) = 1$. Moreover, a representation $k = Q_M(\alpha,\gamma)$ is called primitive (or proper) when $\gcd(\alpha,\gamma) = 1$. We need the following fundamental result from the theory of binary quadratic forms, compare [13, Prop. 4.2].

Fact 9. *Let $n \in \mathbb{N}$ be arbitrary, but fixed. If the binary quadratic form Q_M is primitive, it can primitively represent some integer k that is relatively prime to n.* □

Indeed, when α is the product of all primes that divide n, but not b, and γ the product of all primes that divide n and b, but not c, one sees that $k = Q_M(\alpha,\gamma)$ is an integer that is relatively prime to n.

Remark 10. When the quadratic form Q_M fails to be primitive, its discriminant $\varDelta$ is the product of $(\mathrm{mgcd}(M))^2$ with the discriminant $\varDelta'$ of the 'primitive part' of Q_M. Using (28), this relates to the following property of the eigenvalues $\lambda_{\pm}$ of M, which are the roots of (25):

$$\lambda_{\pm} \, = \, \frac{1}{2}\bigl(T \pm \sqrt{T^2-4D}\,\bigr) \, = \, \frac{1}{2}\bigl(T \pm \sqrt{\varDelta}\,\bigr) \, = \, \frac{1}{2}\bigl(T \pm \mathrm{mgcd}(M)\sqrt{\varDelta'}\,\bigr) \, = \, \frac{1}{2}\bigl(T \pm S\sqrt{\varDelta''}\,\bigr).$$

In the last equality, $\varDelta''$ is the square free part of $\varDelta$, highlighting that $\mathrm{mgcd}(M)|S$. In particular, $\mathrm{mgcd}(M) = 1$ when $\varDelta$ itself is square free. The approach of [32] to studying the dynamics of $\mathrm{GL}(2,\mathbb{Z})$ matrices on L_n involves relating it to the multiplication of the eigenvalue λ_+ on an associated ideal. The latter is an order in a quadratic number field, but generally not its maximal order; see [11, Ch. 2] and [43] for details on the connection between quadratic forms and orders in number fields. ◊

4.3. **Complete determination of local conjugacy.** We now give a complete description of the local conjugacy problem, in the sense of Definition 1. This makes use of a particular normal form over the ring $\mathbb{Z}_n$, with a sequence of elementary arguments.

Proposition 4. *Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ be a matrix with $\mathrm{mgcd}(M) = \mu \neq 0$, and let C be the corresponding companion matrix, as in (24). Then, for all integers $n \geq 2$ that are relatively prime with μ, the reductions of the matrices M and C mod n are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate. In this case, M and C share the same local statistics on L_n.*

Proof. With $\mathrm{mgcd}(M) = \mu$, the integer quadratic form $\frac{1}{\mu} Q_M$ is primitive. By Fact 9, we can thus find $\alpha, \beta \in \mathbb{Z}$ with $\gcd(\alpha,\beta) = 1$ and $\frac{1}{\mu} Q_M(\alpha,\beta) = k$ where k is an integer relatively prime with n. So, $Q_M(\alpha,\beta) = k\mu$, which is still relatively prime with n by assumption.

This means that there is a matrix $A \in \mathrm{Mat}(2,\mathbb{Z})$ with $\det(A) = k\mu$ whose reduction mod n is an element of $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$. Consequently, it defines a conjugacy of M and C on $\tilde{L}_n$, again when taking all matrices mod n. The final claim is clear from Fact 7. □

Note that we need not consider the trivial lattice, $L_1 = \{0\}$, as the point $x = 0$ is fixed by all matrices.

Example 5. The conjugation in Proposition 4 need not be $\mathrm{SL}(2,\mathbb{Z}_n)$-conjugacy, that is, the conjugating element need not have determinant 1 (mod n). To illustrate this, consider the matrices

$$M = \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix},$$

with $D = -2$, $T = 4$ and, from (27), quadratic form $Q_M(\alpha,\gamma) = 2\alpha^2 - 3\gamma^2$ (primitive since $\mathrm{mgcd}(M) = 1$). Over $\mathbb{Z}_3$, the quadratic form reduces to $2\alpha^2$, which can represent 0 and 2, but never 1, so that M and C are not conjugate over $\mathrm{SL}(2,\mathbb{Z}_3)$. This example highlights that the approach of [5] is of limited value for our problem. ♢

The following result is obvious from Proposition 4, because $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugacy induces a graph isomorphism in the sense of Definition 1, compare Fact 7.

Corollary 2. *Let M, M' be two integer matrices with the same trace and determinant, whence they share the same companion matrix. If, in addition, $\mathrm{mgcd}(M') = \mathrm{mgcd}(M) = 1$, the toral endomorphisms defined by M and M' have the same local statistics on all lattices L_n.* □

Example 6. Let us briefly return to the matrices M, M^{-1} and C of Example 4. They all have mgcd $= 1$, but are in different $\mathrm{GL}(2,\mathbb{Z})$ conjugacy classes. Nevertheless, Corollary 2 shows they all give the same local statistics, on all lattices L_n. The same conclusion applies to the matrices M and M' of Example 3. ♢

Let us proceed to the general case when $\mathrm{mgcd}(M) = r \geq 1$ from the point of view of local conjugacies. Consider the matrix M from (20), and let $r = \mathrm{mgcd}(M)$. We may now decompose M as

$$M \, = \, a\mathbb{1} + rN \quad \text{with} \quad N \, = \, \begin{pmatrix} 0 & \tilde{b} \\ \tilde{c} & (d-a)\tilde{} \end{pmatrix}. \tag{29}$$

When $r = 0$, we have the trivial case $M = a\mathbb{1}$, which we now put aside by assuming $r \in \mathbb{N}$, in line with Fact 8, so that $\operatorname{mgcd}(N) = 1$ by construction.

Proposition 5. *Let* $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *be an integer matrix with* $\operatorname{mgcd}(M) = r \neq 0$. *Then, for all integers* $n \geq 2$, *and when taking all matrices mod* n, M *is* $\operatorname{Mat}(2, \mathbb{Z}_n)^{\times}$*-conjugate to the integer matrix* $\left(\begin{smallmatrix} a & bc/r \\ r & d \end{smallmatrix}\right)$.

Proof. By construction, the matrix N in the decomposition (29) is still an integer matrix, with $\operatorname{mgcd}(N) = \gcd\bigl(\tilde{b}, \tilde{c}, (d-a)\tilde{}\,\bigr) = 1$. By Proposition 4, for all integers $n \geq 2$, N is then $\operatorname{Mat}(2, \mathbb{Z}_n)^{\times}$-conjugate to its companion matrix

$$C_N = \begin{pmatrix} 0 & \tilde{b}\,\tilde{c} \\ 1 & (d-a)\tilde{} \end{pmatrix},$$

where both N and C_N are taken mod n.

The claim now follows from the observation that this conjugacy extends to the one claimed by the structure of the decomposition $M = a\mathbb{1} + rN$. Indeed, the relation $N = AC_N A^{-1}$ together with (29) immediately implies $AMA^{-1} = a\mathbb{1} + rC_N$. □

It is worth recalling that [12, Lemma 1] does not apply to 2×2-matrices, meaning that we do not have global conjugacy in general. The benefit of Proposition 5 is that we obtain a local conjugacy instead, and to a matrix with a well-defined element in the lower left corner. For the further arguments, we need a technical result, formulated within $\operatorname{Mat}(2, \mathbb{Z})$, hence *prior* to looking at the reductions mod n.

Lemma 3. *Let* $M, M' \in \operatorname{Mat}(2, \mathbb{Z})$ *be the two matrices of* (20) *and assume that* $\det(M) = \det(M') = D$ *and* $\operatorname{tr}(M) = \operatorname{tr}(M') = T$. *Assume, in addition, that* $\operatorname{mgcd}(M) = \operatorname{mgcd}(M') = r \in \mathbb{N}$. *Then,* r *divides* $d - d'$.

Proof. When $d = d'$, the statement is trivially true, so we may assume that $d \neq d'$. Since $r = \gcd(b, c, d-a) = \gcd(b', c', d'-a')$, one has $r^2 | bc$ and $r^2 | b'c'$. Observe that

$$(a - d')(d - d') \;=\; ad + (d' - T)d' \;=\; ad - a'd' \;=\; D + bc - D - b'c' \;=\; bc - b'c',$$

which implies that $r^2 | (a-d')(d-d')$. With $m := d - d' \neq 0$ and $d - a = kr$, where $k \in \mathbb{Z}$ by assumption, we now have to consider

$$r^2 \mid m(m - kr) \tag{30}$$

and to show that this implies $r|m$. When $m = kr$, this is again clear, so assume $m - kr \neq 0$. Then, let $r^2 = p_1^{2s_1} \cdot \ldots \cdot p_\ell^{2s_\ell}$ be the unique prime decomposition of r^2 into powers of distinct primes. Let t_i be the highest power so that $p_i^{t_i} | m$, which is a non-negative integer.

Assume that $t_i < s_i$ for some index i. By (30), this implies $p_i^{2s_i - t_i} | (m - kr)$ and thus, as $p_i^{s_i} | r$ and $2s_i - t_i > s_i$, also $p_i^{s_i} | m$, in contradiction to the assumption that $t_i < s_i$. Consequently, we must indeed have $t_i \geq s_i$ for all $1 \leq i \leq \ell$. Since $r = \prod_i p_i^{s_i}$, this means that $r|m$ as claimed. □

Proposition 6. *Let* M, M' *be the matrices from* (20) *and assume that they have the same trace and determinant. Assume further that* $\operatorname{mgcd}(M) = \operatorname{mgcd}(M') = r$. *Then, for an* *arbitrary integer $n \geq 2$, the reductions mod n of the matrices M and M' are* $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$*-conjugate.*

Proof. When $r = 0$, Fact 8 implies $M = M'$. So, let us assume $r \in \mathbb{N}$. By Proposition 5, we know that matrices M and M' are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate to integer matrices N and N', where

$$N = \begin{pmatrix} a & \frac{b\,c}{r} \\ r & d \end{pmatrix} \quad \text{and} \quad N' = \begin{pmatrix} a' & \frac{b'c'}{r} \\ r & d' \end{pmatrix},$$

in the sense that their reductions mod n satisfy the corresponding conjugacies. Our claim follows if we can show that also N and N' are $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugate in this sense.

Consider the unimodular matrix $A = \left(\begin{smallmatrix} 1 & \frac{d-d'}{r} \\ 0 & 1 \end{smallmatrix}\right)$, which is an integer matrix by Lemma 3 and hence an element of $\mathrm{GL}(2,\mathbb{Z})$. Using $\mathrm{tr}(M) = \mathrm{tr}(M')$ and $\det(M) = \det(M')$, it is easy to check that $AN = N'A$ holds, hence $N' = ANA^{-1}$ within $\mathrm{GL}(2,\mathbb{Z})$. By Fact 6, this implies the local conjugacy claimed. □

Let us investigate the local conjugacies a bit further, aiming at a converse of Proposition 6.

Proposition 7. *Let $M, M' \in$ $\mathrm{Mat}(2,\mathbb{Z})$ be two integer matrices whose reductions mod n are* $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$*-conjugate for some $n \geq 2$. Then, M and M' have the same determinants and traces mod n, and their matrix gcds r, r' generate the same ideal in $\mathbb{Z}_n$, meaning $r\mathbb{Z}_n = r'\mathbb{Z}_n$.*

Proof. The statement about the determinants and traces is clear. For the claim about the matrix gcd, we can again use the idea of the proof of Lemma 2, up to the point where we conclude that $r|r'$ and $r'|r$, now seen as divisibility properties within $\mathbb{Z}_n$. But $k|\ell$ means that the principal ideal $(\ell) = \ell\mathbb{Z}_n$ is contained in (k), so that we obtain $(r) \subset (r')$ and $(r') \subset (r)$, hence $(r) = (r')$. □

At this stage, one can formulate the following central result.

Theorem 2. *For two integer matrices $M, M' \in$ $\mathrm{Mat}(2,\mathbb{Z})$, the following statements are equivalent:*

(a) *The reductions mod n of M and M' are* $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$*-conjugate for all $n \geq 2$;*
(b) *M and M' satisfy the three relations* $\det(M) = \det(M')$, $\mathrm{tr}(M) = \mathrm{tr}(M')$ *and* $\mathrm{mgcd}(M) = \mathrm{mgcd}(M')$.

Proof. The direction (b) $\Longrightarrow$ (a) follows directly from Proposition 6.

For the converse direction, we may conclude from Proposition 7 that $\det(M) \equiv \det(M')$ mod n and $\mathrm{tr}(M) \equiv \mathrm{tr}(M')$ mod n for all $n \geq 2$. Consequently, we must have $\det(M) = \det(M')$ and $\mathrm{tr}(M) = \mathrm{tr}(M')$ (recall that $k \equiv \ell \bmod n \in \mathbb{N}$ means that $k - \ell$ is divisible by n, which simultaneously holds for all $n \in \mathbb{N}$ only when $k - \ell = 0$).

For the third identity, let $r = \mathrm{mgcd}(M)$ and $r' = \mathrm{mgcd}(M')$ and assume that $r\mathbb{Z}_n = r'\mathbb{Z}_n$ for all $n \geq 2$, but $r \neq r'$. Consequently, there is a prime p with $r = p^s \varrho$ and $r' = p^t \varrho'$, $t \neq s$, such that ϱ and ϱ' are both relatively prime with p. Without loss of generality, we may assume that $t > s$, and then choose $n = p^t$. Clearly, both ϱ and ϱ' are then units in $\mathbb{Z}_n$ by construction. With $(r) := r\mathbb{Z}_n$, we then obtain $(r) = (p^t \varrho) = (p^t) = (0)$, while $(r') = (p^s \varrho') = (p^s) \neq (0)$, in contradiction to the original assumption. □

This theorem permits the following answer to the question for the local statistics of an integer matrix.

Corollary 3. *The complete local statistics of an integer matrix M, in the sense of Definition 1, only depends on the three invariants* $\det(M)$, $\mathrm{tr}(M)$ *and* $\mathrm{mgcd}(M)$. *Two integer matrices with the same triple of invariants thus have the same local statistics on all lattices L_n. In particular, they have the same fixed point counts, both locally and globally.* □

The result of Theorem 2 permits an interpretation in terms of $\widehat{\mathbb{Z}}$, which is the inverse (or projective) limit of the rings $\mathbb{Z}_n$ over the positive integers ordered by divisibility, written as $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}_n$. It is also known as the Prüfer ring, see [30] for details.

Corollary 4. *In the situation of Theorem 2, any of the two conditions is equivalent to the matrices M and M' being* $\mathrm{GL}(2,\widehat{\mathbb{Z}})$*-conjugate.*

Proof. Clearly, a $\mathrm{GL}(2,\widehat{\mathbb{Z}})$-conjugacy implies condition (a) of Theorem 2. Conversely, assuming (a), consider the inverse system of $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-subsets $X(n)$ defined by

$$X(n) = \{A \in \mathrm{Mat}(2,\mathbb{Z}_n)^{\times} \mid AM = M'A\}$$

with $n \in \mathbb{N}$ and ordered inductively by divisibility. All $X(n)$ are non-empty by assumption and finite. Let $X = \varprojlim X(n)$ be the inverse limit, which is then non-empty as well. Any element in X achieves the required conjugacy via the corresponding projections. □

We conclude by noting:

Remark 11. One consequence of Theorem 2 for $\mathrm{SL}(2,\mathbb{Z})$ matrices, noting (23), is that such a matrix is conjugate to its inverse on *all* lattices individually, despite the fact that this is generally untrue on the torus, as in Example 4. This relates to the investigations of quantum cat maps and their perturbations in [25]. ◊

Remark 12. We have described the three invariants for complete $\mathrm{Mat}(2,\mathbb{Z}_n)^{\times}$-conjugacy, whereas [3] presented the analogous result for $\mathrm{GL}(2,\mathbb{Z})$-conjugacy. The conjugacy of M and M' in the special linear group over the p-adic integers is a related question, addressed in [5], though Example 5 above indicates the difference to $\mathrm{GL}(2,\mathbb{Z}_n)$-conjugacy. ◊

Acknowledgements

It is a pleasure to thank Grant Cairns, Natascha Neumärker, Franco Vivaldi, Benjy Weiss and Peter Zeiner for discussions and useful hints on the manuscript. This work was supported by the German Research Council (DFG), within the CRC 701, and under the Australian Research Council's Discovery funding scheme (project number DP 0774473), including mutual visits.

References

[1] R. L. Adler and R. Palais, *Homeomorphic conjugacy of automorphisms of the torus*, Proc. AMS **16** (1965) 1222–1225.

[2] R. L. Adler and B. Weiss, *Entropy, a complete metric invariant for automorphisms of the torus*, Proc. Nat. Acad. Sci. USA **57** (1967) 1573–1576.

[3] R. Adler, C. Tresser and P. A. Worfolk, *Topological conjugacy of linear endomorphisms of the 2-torus*, Trans. AMS **349** (1997) 1633–1652.

[4] H. Appelgate and H. Onishi, *Continued fractions and the conjugacy problem in* $\mathrm{SL}(2,\mathbb{Z})$, Commun. Algebra **9** (1981) 1121–1130.

[5] H. Appelgate and H. Onishi, *Similarity problem over* $SL(n,\mathbb{Z}_p)$, Proc. AMS **87** (1983) 233–238.

[6] M. Baake, J. Hermisson and P. A. B. Pleasants, *The torus parametrization of quasiperiodic LI-classes*, J. Phys. A: Math. Gen. **30** (1997) 3029–3056; `mp_arc/02-168`.

[7] M. Baake and J. A. G. Roberts, *Reversing symmetry group of* $\mathrm{GL}(2,\mathbb{Z})$ *and* $\mathrm{PGL}(2,\mathbb{Z})$ *matrices with connections to cat maps and trace maps*, J. Phys. A: Math. Gen. **30** (1997) 1549–1573.

[8] M. Baake and J. A. G. Roberts, *Symmetries and reversing symmetries of toral automorphisms*, Nonlinearity **14** (2001) R1–R24; `arXiv:math.DS/0006092`.

[9] J. Banks, J. Brooks, G. Cairns, G. Davis, and P. Stacey, *On Devaney's definition of chaos*, Amer. Math. Monthly **99** (1992) 332–334.

[10] E. Behrends and B. Fiedler, *Periods of discretized linear Anosov maps*, Ergod. Th. & Dynam. Syst. **18** (1998) 331–341.

[11] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York (1966).

[12] J. L. Brenner, *The linear homogeneous group III*, Ann. Math. **71** (1960) 210–223.

[13] D. A. Buell, *Binary Quadratic Forms – Classical Theory and Modern Computations*, Springer, New York (1989).

[14] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York (1962).

[15] M. Degli Esposti and S. Isola, *Distribution of closed orbits for linear automorphisms of tori*, Nonlinearity **8** (1995) 827–842.

[16] M. Degli Esposti and B. Winn, *The quantum perturbed cat map and symmetry*, J. Phys. A: Math. Gen. **38** (2005) 5895–5912.

[17] F. J. Dyson and H. Falk, *Period of a discrete cat mapping*, Amer. Math. Monthly **99** (1992) 603–614.

[18] F. Faure, S. Nonnenmacher and S. De Bièvre, *Scarred eigenstates for quantum cat maps of minimal periods*, Commun. Math. Phys. **239** (2003) 449–492.

[19] G. Gaspari, *The Arnold cat map on prime lattices*, Physica **73D** (1994) 352–372.

[20] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, reprint, Dover, New York (2004).

[21] J. H. Hannay and M. V. Berry, *Quantization of linear maps on the torus – Fresnel diffraction by a periodic grating*, Physica **1D** (1980) 267–290.

[22] H. Hasse, *Number Theory*, Springer, Berlin (1980).

[23] A. Katok and B. Hasselblatt, *Introduction to the Modern Theory of Dynamical Systems*, Cambridge University Press, Cambridge (1995).

[24] J. P. Keating, *Asymptotic properties of the periodic orbits of the cat maps*, Nonlinearity **4** (1991) 277–307.

[25] J. P. Keating and F. Mezzadri, *Pseudo-symmetries of Anosov maps and spectral statistics*, Nonlinearity **13** (2000) 747–775.

[26] P. Kurlberg, *On the order of unimodular matrices modulo integers*, Acta Arith. **110** (2003) 141–151.

[27] P. Kurlberg and Z. Rudnick, *Hecke theory and equidistribution for the quantization of linear maps of the torus*, Duke Math. J. **103** (2000) 47–77.

[28] P. Kurlberg and Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Commun. Math. Phys. **222** (2001) 201–227.

[29] S. Lang, *Algebra*, rev. 3rd ed., Springer, New York (2002).

[30] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin (1999).

[31] N. Neumärker, *Orbitstatistik und relative Realisierbarkeit*, Diploma Thesis, Univ. Bielefeld (2007).

[32] I. Percival and F. Vivaldi, *Arithmetical properties of strongly chaotic motions*, Physica **25D** (1987) 105–130.

[33] Y. Puri and T. Ward, *Arithmetic and growth of periodic orbits*, J. Integer Sequences **4** (2001) 01.2.1

[34] H. Rademacher, *Zur Theorie der Dedekindschen Summen*, Math. Z. **63** (1956) 445–463; see also MR 0079615 by H. D. Kloosterman for a short summary.

[35] J. A. G. Roberts and M. Baake, *Trace maps as 3D reversible dynamical systems with an invariant*, J. Stat. Phys. **74** (1994) 829–888.

[36] D. Ruelle, *Dynamical Zeta Functions for Piecewise Monotone Maps of the Interval*, CRM Monograph Series, vol. 4, AMS, Providence, RI (1994).

[37] P. Seibt, *A period formula for torus automorphisms*, Discr. Cont. Dynam. Syst. **9** (2003) 1029–1048.

[38] N. J. A. Sloane, *The Online Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/

[39] S. Smale, *Differentiable dynamical systems*, Bull. AMS **73** (1967) 747–817.

[40] O. Taussky, *Introduction into connections between algebraic number theory and integral matrices*, appendix to: H. Cohn, *A Classcial Invitation to Algebraic Numbers and Class Fields*, Springer, New York (1978), pp. 305–321.

[41] P. Walters, *An Introduction to Ergodic Theory*, reprint, Springer, New York (2000).

[42] T. Ward, *Exactly realizable sequences*, http://www.mth.uea.ac.uk/~h720/research/files/integersequences.html

[43] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin (1971).

Fakultät für Mathematik, Universität Bielefeld,
Postfach 100131, 33501 Bielefeld, Germany
E-mail address: mbaake@math.uni-bielefeld.de
URL: http://www.math.uni-bielefeld.de/baake

School of Mathematics and Statistics, University of New South Wales,
Sydney, NSW 2052, Australia
E-mail address: jag.roberts@unsw.edu.au
URL: http://www.maths.unsw.edu.au/~jagr

Department of Mathematical and Statistical Sciences, University of Alberta,
Edmonton, AB, Canada T6G 2G1
E-mail address: aweiss@math.ualberta.ca
URL: http://www.math.ualberta.ca/Weiss_A.html